Public key infrastructure

Technology, Information Technology

Public Key Infrastructure Case Overview The organization is presently using a Microsoft Server Active Directory domain which is administered bya team of information security. The management is convinced to implement Public Key Infrastructure (PKI) as a framework to ensure integrity, confidentiality, nonrepudiation and authentication in their operation. Subsequently, the company would be using digital certificate to sign software to demonstrate authenticity of software to their clients. With this regard the study focuses on analyzing the fundamentals of PKI and their application in order to ensure quality resources within the organization.

Discussion

PKI is set of complex set of application that supports other application system and components that will assist in building a network security. Implementation of PKI is anticipated to serve as an essential component of an overall security system within the organization (Zao, 2012; Hanka et al., 2011). PKI is highly scalable and helps the in maintaining certificates with their unique identity. A feature of PKI such as scalability further creates no requirement of third party authentication. Through the feature of the delegation of trust the software enhances the authentication of the software within the end users. To enhance the security system within an organization the PKI provides unique codes and ensures that only legitimate users are able to access to the system resources. These features of PKI along with identity based self-certified keys are anticipated to ensure better security system controlled within the organization (The Saylor Foundation, 2012). PKI system allows the use of mathematically related key pairs, to be used for public and private level. The private key is used to safeguard the

requirement of the privacy at the organizational level. Correspondingly, the public keys provide a unique identification to the users of the software. This method of encryption and decryption is further observed to help the organization to authenticate the software and enhances the credibility to the customers (United States Department of Agriculture, n. d.).

The certificate authority helps in creating and binding the public encryption keys. The in-house certification authority enhances the maximum level of control over the different software being used within an organization. The process employs a digital sign which enhances the financial soundness, liability protection as well as enhances the corroboration of transaction. The document that is signed by a trusted b y a third party organization is referred to as a public Certificate Authority (CA). The in-house CA has been the most trusted type of the security system but are also very costly at the same time. The public CA is based on the policy module depended on the predefined list of certificate extensions. However, by sharing of the certificate encryption among the public CAs increases its vulnerability and enhances the chances of being hacked. On the other hand the public CA enhances the security of the public websites and in turn enhances the transparency of the data reducing their vulnerability. This helps the organization to increase their security system and also ensures their development of the certificate authority by reducing vulnerabilities related to security aspect (Preneel, 2011). Based on the above stated factors, it is proposed to the organization to use public CA as it is less costly while it is also effective enough to guarantee adequate security (Hanka et al., 2011).

Conclusion

The organization should be implementing the PKI in order to reduce the any possible security threats within the organization. Moreover by implementing the PKI, the organization will be able to increase their integrity and credibility that would facilitate it to acquire the greater confidence of the end users. By issuing the digital certificates the company will be able to ensure their authentication and non-repudiation at a larger extent.

References

Hanka, O., Eichhorn, M., Pfannenstein, M., Eberspacher, J. & Steinbach, E. (2011). A distributed public key infrastructure based on threshold cryptography for the Hiimap next generation internet architecture. Future Internet, 3, 1-5.

Preneel, B. (2011). Public key infrastructure fundamentals. Katholieke Universiteit Leuven, 1-30.

The Saylor Foundation. (2012). Public key infrastructure. Retrieved from http://www. saylor. org/site/wp-content/uploads/2012/07/Public-key-infrastructure1. pdf

United States Department of Agriculture. (2013). Use of public key infrastructure (PKI). Retrieved from http://www. ocio. usda. gov/sites/default/files/docs/2012/DM3530-003. htm

Zao, J. K. (2012). Public key infrastructure (PKI). Computer Science Department, 1-17.